Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

LABMD, INC., Plaintiff, v. TIVERSA HOLDING CORP. f/k/a TIVERSA, INC.; ROBERT J. BOBACK~~; M. ERIC JOHNSON~~; and DOES 1-10, Defendants.	**No. 2:15-cv-**00092-MRH-MPK **ELECTRONICALLY FILED** **JURY TRIAL DEMANDED**

FIRST AMENDED COMPLAINT[1]

[Deleted]

Plaintiff LabMD, Inc. ("Plaintiff" or "LabMD"), by and through counsel, files~~brings~~ this First Amended Complaint~~action~~ against Defendants Tiversa Holding Corp. f/k/a Tiversa, Inc. ("Tiversa"), Robert J. Boback ("Boback"), ~~M. Eric Johnson ("Johnson")~~ (collectively, Tiversa and~~,~~ Boback~~, and Johnson~~ are referred to as "Defendants"), and DOES 1-10, pursuant to the Court's January 8, 2016 Memorandum Order (ECF No. 115)[2] and alleges the following:

NATURE OF THE ACTION

1. This is an action to recover millions of dollars in damages that Defendants intentionally caused to LabMD, through a multi-year, nationwide, continuing ~~racketeering~~

[1] For the convenience of the Court and all parties, Exhibit A hereto is a redlined version of LabMD's First Amended Complaint.

[2] In furtherance of the Court's Memorandum Order, LabMD does not include in this amendment its original Counts I, VII or VIII or any claims against Defendant M. Eric Johnson, said claims having been dismissed by the Court with prejudice. LabMD reserves any and all appeal and other rights with respect to those claims. To the extent there are allegations in the original complaint and exhibits thereto and LabMD's RICO Statement and exhibits thereto, those allegations are incorporated herein.

scheme and conspiracy, which decimated LabMD, a privately owned cancer testing facility. At its peak, LabMD employed approximately 40 medical professionals, but, as a result of Defendants' actions, it is now nothing more than an insolvent shell of a company.

2. ~~In the past year,~~ Boback, Tiversa's Chief Executive Officer, has admitted to Congress and/or the FTC that Defendants: (i) lied about the source of LabMD's alleged data security breach, and (ii) lied by saying that they had detected purported identity thieves downloading LabMD's files from the internet. While LabMD has always believed that it was treated poorly by Defendants, it did not know until Boback's recent admissions that Defendants had made these material misrepresentations.

3. Defendants, led by Boback, designed their scheme for the purpose of commercially benefitting from the fear mongering that stemmed from privacy and data security breaches, some of which were of their own creation. As former FTC Commissioner J. Thomas Rosch once explained: Tiversa "is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations." (*See* Dissenting Statement of Commissioner J. Thomas Rosch, a true and correct copy of which is attached to the original complaint as Exhibit "A" and is incorporated herein.~~hereto as Exhibit "A"~~).

4. In the instant matter, Tiversa, at Boback's direction, hacked into LabMD's computer in Georgia, and then attempted to sell LabMD services to remedy the very breach Tiversa created. Tiversa first spun a yarn about identity thieves downloading LabMD's client data from the internet and then analogized to the "widely reported file sharing breach of Supreme Court Justice Stephen Breyer's SSN and personal data." (*See* July 15, 2008 email from

Boback to LabMD, a true and correct copy of which is attached ~~hereto~~ to the original complaint as Exhibit "B" and is incorporated herein.~~as Exhibit "B"~~). When LabMD refused to purchase Tiversa's services, Defendants turned LabMD in to the FTC (for the very breach Tiversa created), and then used LabMD's client files as the subject of Defendants' report about data security.

5. Defendants' scheme has employed various fraudulent and otherwise tortious methods, including: making misrepresentations to LabMD, the FTC, Congress, the media, and the public; converting LabMD's property, and; defaming LabMD. Defendants engaged in this scheme to directly target and harm LabMD.

PARTIES

6. Plaintiff is a corporation organized and existing under the laws of the state of Georgia with its principal place of business located in Fulton County, Georgia.

7. Defendant Tiversa is a corporation organized and existing under the laws of the state of Delaware with its principal place of business at 606 Liberty Avenue, Pittsburgh, Allegheny County, Pennsylvania 15222. Tiversa can be served with process through its President, Robert Boback, at 606 Liberty Avenue Pittsburgh, PA 15222, or wherever he may be found.

8. Defendant Boback is an individual citizen of the state of Pennsylvania, is over the age of 18, and can be served with process at 606 Liberty Avenue Pittsburgh, PA 15222, or wherever he may be found. Boback is sued in his individual capacity as well as his capacity as the chief executive officer of Tiversa.

9. [Deleted.]

10. DOE Defendants 1-10 are and were, at all relevant times, citizens of the United States; are as-yet unidentified individuals or entities that actively participated in and/or materially benefitted from the illicit conduct detailed herein; and will be substituted with the proper names of these individuals or entities as they become available.

JURISDICTION AND VENUE

11. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332 in that (a) it is between citizens of different states, and (b) the matter in controversy exceeds $75,000, exclusive of interest and costs.

12. Defendants Tiversa and Boback are subject to the jurisdiction of this Court because they are citizens of the state of Pennsylvania. [Remainder deleted from original Complaint].

13. Venue for this action lies in this judicial district and division pursuant to 28 U.S.C. § 1391(b).

FACTS

14. [Deleted.]

15. [Deleted.]

16. [Deleted.]

17. [Deleted.]

18. [Deleted.]

19. [Deleted.]

20. [Deleted.]

21. [Deleted.]

22. [Deleted.]

23. [Deleted.]

24. [Deleted.]

25. [Deleted.]

26. [Deleted.]

27. [Deleted.]

28. [Deleted.]

29. [Deleted.]

30. [Deleted.]

31. [Deleted.]

32. [Deleted.]

33. [Deleted.]

34. [Deleted.]

35. [Deleted.]

36. [Deleted.]

37. [Deleted.]

Peer-to-Peer Networks

14. A peer-to-peer ("P2P") network is created when two or more computers are connected and share resources without going through a separate central server computer.

15. The only requirements for a computer to join a P2P network are an internet connection and P2P software. Common P2P software programs have included Kazaa, Limewire, BearShare, Morpheus, Bit Torrent and eMule. These software programs connect to one or more of the P2P networks. Such networks have included Gnutella, G2 and eDonkey.

16. The purpose of most P2P networks is to search for, identify and share files stored on computers (*e.g.,* music, video, pictures, PDFs). P2P software typically allows users to share files only within a single folder on their computer that has been designated for sharing.

17. P2P software programs enable one computer to search a limited number of other computers for all files that have been made available for sharing by other computer users, so long as the other computers are also using the file-sharing application and are within the radius of the search.

18. Users of peer-to-peer networks perform searches using terms related to the particular file they hope to find. In response, they receive a list of possible matches, if any matches are made. The user then chooses a file they want to download from the list.

19. The search capabilities on peer-to-peer networks are limited. P2P networks use portions of the internet to connect a limited number of computers to each other but they are not *the* internet and they do not work like the internet. P2P networks, for example, are not designed for and do not use search engines like Google. They are not designed to handle large amounts of traffic and they are specifically designed to *limit* each search to a *limited* number of computers within a defined radius.

20. P2P networks are only capable of searching for computer files by their filenames. These networks do not have the capability for users to search for files using words or other data contained *in* the files for which the user is searching. In addition, search terms on P2P networks must be precise. With LimeWire, for example, a user searching for files with the search terms "insurance" and "aging" would not find any insurance aging files with the filename "insuranceaging."

21. P2P software allows searching and retrieval of computer files directly through firewalls through a technique called "pushing." A push is a request that (1) is initiated by a computer outside of a firewalled computer, (2) is sent to the firewalled computer through normal inbound connections and (3) utilizes programming in the firewalled computer to "push" files through outbound connections that are usually not protected. A push request causes the firewall to "think" that a computer behind the firewall actually wants the firewall to let one or more of its files through.

22. In P2P networks, folders designated for sharing files often contain computer files that no one ever intended to share. Many computer users do not know when or if the computer they are using is loaded with P2P software. Most computer users would not even know to ask. Thus, in a variety of settings, computer users may accidentally, unintentionally, unknowingly and/or inadvertently place computer files in a computer folder they did not know was designated (*e.g.,* by a child, a former computer owner, a former employee or malware) for sharing.

Tiversa's Pseudonode Technology

23. Peers (*i.e.*, computers) on P2P networks are also called nodes. Tiversa developed and uses proprietary technologies that search for and download massive amounts of data from multiple peer-to-peer networks all across the world. Ordinary users of P2P networks do not have such capabilities. In fact, Tiversa may be the only company in the world with such capabilities.

24. In the hands of an irresponsible company or irresponsible people, this technology is extremely dangerous to individuals, companies, governments, states, nations and countries. This lawsuit results from the fact that Tiversa, its officers, its directors, several of its employees and its advisory board have all been irresponsible with Tiversa's technologies, resources and expertise.

25. Tiversa's technologies are largely based on electronic deceit and trickery. Tiversa's technologies utilize a combination of components in P2P networks known as true nodes and "pseudonodes." Pseudonodes, also known as "rogue" nodes and "fake" nodes, are nodes that can be configured to trick P2P networks in a variety of ways, some of which are quite nefarious. For example, according to Tiversa's patents, a Tiversa pseudonode can be configured to:

- connect to thousands of true network nodes on multiple networks (as opposed to actual network nodes which are limited to one to ten connections);
- detect, store and manage the IP and network addresses of the true network nodes to which it is connected;
- record search requests initiated by others, to capture the responding information and to intercept a copy of files requested by others;
- impersonate a true network nodes;
- impersonate multiple true network nodes;
- dynamically change its IP address to a fake or real IP address;
- falsify its client ID;
- falsify its GUID;
- use a configured list of fake addresses or a single fake address generated at random. If an address does not actually appear on a network, a Tiversa pseudonode can make it appear as though it does;
- generate and send false search responses, each with a different IP address and client ID to make it appear that the requested information has spread to multiple nodes;

- generate and send false search responses that contain random file names and file sizes from random network nodes;

- generate and send false search responses that contain the same file with different file sizes;

- accept a search request from a true network node and replace the search string with a random set of falsified numbers and characters but keep the same message ID;

- eliminate searches from the network;

- send a response that causes the originator of the search to cease to function or severely limit its operation;

- respond to searches with incorrect information; and

- generate and send a false response that fills a user's monitor with irrelevant information.

26. Normal P2P network users do not know when their transmissions are being tapped, intercepted and/or manipulated by Tiversa's technologies. Moreover, normal P2P network users are not able to prevent Tiversa's technologies from interfering with, spying on and/or capturing their transmissions.

27. Tiversa does not seek permission to access others' computers, to view or listen to others' computer files or download and keep computer files that it knows are owned by other people. Every week, Tiversa finds and downloads into its database millions of files that individuals, companies and governments never intended to share and never authorized Tiversa to

see or take. Tiversa regularly claims that all of the files it downloads have been made publicly available in some fashion. This is a façade. It is entirely false.

28. Tiversa is particularly interested in finding and downloading personal and private information such as individual tax returns, medical records, social security numbers, credit card numbers, personal identifying information ("PII"), personal health information ("PHI") passwords, financial accounts, investment accounts and banking statements ("Private Files"). Tiversa also searches for and downloads confidential information on corporate executives, corporate operations, corporate financials, sales, legal matters, employment records, trade secrets, competitively sensitive and privileged information ("Confidential Files"). In addition, Tiversa searches for and downloads classified information relating to the Department of Homeland Security, the Central Intelligence Agency, the Federal Bureau of Investigation, the National Security Administration, military personnel, major military commands, military government contractors and military operations. ("Classified Files").

29. Tiversa specifically searches for and collects Private Files, Confidential Files and Classified Files without permission or authority from the owners of the computers they hack, the owners of the files they take or the individuals, companies and governments who have personal, proprietary and national security interests in the data contained in those files.

30. There are state and federal laws designed to prevent this kind of information gathering and storage. *See, e.g.*, 18 Pa.C.S. § 7611 (Unlawful use of computer and other computer crimes); O.C.G.A. § 16-9-93 (Computer crimes defined; exclusivity of article; civil remedies; criminal penalties); 18 U.S. Code § 1030 (Fraud and related activity in connection with computers); 42 U.S.C. § 1320d-6 (Wrongful disclosure of individually identifiable health information); 18 U.S. Code § 798 (Disclosure of classified information); 18 U.S.C. §§ 1462,

1466, 1466A, 2252, 2252A (Child pornography); 18 U.S. Code § 793 (Gathering, transmitting or losing defense information); 18 U.S. Code § 1924 (Unauthorized removal and retention of classified documents or material); 18 U.S. Code § 1832 (Theft of trade secrets); 18 Pa.C.S. § 3930 (Theft of trade secrets); and O.C.G.A. § 16-8-13 (Theft of trade secrets); *see also* various state laws regarding the unlawful possession of personal identifying information, including, without limitation, Ariz. Rev. Stat. Ann. §13-2008; Colo. Rev. Stat. §18-5-903.5, 904 and 905; Fla. Stat. §817.5685; Hawaii Rev. Stat. §708-839.55; La. Rev. Stat. Ann. §14:70.7; Nev. Rev. Stat. §205.465; N.Y. Penal Law §190.81, .82 and .83; and Or. Rev. Stat. §165.810; Tex. Penal Code Ann. §32.51; Utah Code Ann. §76-6-1105.

31. Tiversa monetizes information it obtains from Private Files, Confidential Files and Classified Files either by selling a monitoring contract (pursuant to which Tiversa would search for certain key words for a period of time), or by selling a "one-off" service (which would remediate just the existing disclosure problem). Tiversa typically creates an "incident response" for its "one-off" services.

32. In Tiversa's searches for Private Files, Confidential Files and Classified Files, Tiversa records (1) the information disclosed, (2) the IP address of the disclosing computer, (3) metadata from the file, (4) the identity of the disclosing company and (5) when the information was disclosed. Much of this information is included on spreadsheets that Tiversa analysts update several times a day. The purpose of the spreadsheets is so that Boback and the Tiversa sales force can make sales calls to the affected companies.

33. When contacting affected company to sell services, Tiversa's practice is to (1) explain that, because of a security breach, it found one or more of the company's files on a P2P network, (2) explain that the file or files contain private, confidential and/or classified

information, (3) not reveal the true source of the information, (4) tell the potential customer that Tiversa did not record the IP information and (5) offer its services to fix the potential customer's alleged problem. Tiversa will provide a found document to a potential customer only after stripping the IP address and deceptively altering any metadata relating to the disclosure source, while keeping a copy of the file that includes the files' true disclosure source information.

34. Tiversa fabricates information and documentation regarding the disclosing source of files it finds with its technologies. If a potential customer chooses not to purchase Tiversa's services, Tiversa will often attempt to monetize its findings by notifying an *existing* Tiversa customer of the source of the customer's information and advising the *existing* customer to contact Tiversa's target.

35. When a company refuses to purchase Tiversa's services, Boback often tells his analysts, in reference to that company, to the effect of, "you think you have a problem now, you just wait." In many of these situations, Boback directs Tiversa analysts to manipulate information in Tiversa's database so as to make that company's files "proliferate" and thereby make it appear, falsely, that a file had "spread" to multiple places on P2P networks. Tiversa then uses this "evidence" to follow up with a company to try again to get the company to purchase Tiversa's services.

36. For companies that initially refuse to purchase Tiversa's services, Tiversa often follows up with the target by stating, falsely and fraudulently, that the disclosed document had spread to additional IP addresses, including IP addresses of known "bad actors" or identity thieves. In such cases, Tiversa's analysts have or will alter disclosure, source and spread information in Tiversa's database to make it appear that Tiversa had located and downloaded the

file from the IP address of an identity thief or other bad actor and that the file had proliferated to multiple locations on P2P networks.

37. Because of the nature of Tiversa's technologies and the irresponsible officers, directors, employees and advisory board members at the company, Tiversa and Boback not only commit fraud on a regular basis, they are also very effective at concealing their fraud. Whenever Tiversa falsely claims that a company's computer files (1) were disclosed from a particular source, (2) spread to other computers on a P2P network or (3) were found on computers of known identity thieves and bad actors, Tiversa is able to conceal these frauds because there are no other technologies to utilize or companies to hire to disprove their fraudulent claims. Moreover, Tiversa makes a concerted effort to conceal their frauds by manipulating data in their database.

Tiversa's Theft of LabMD's File

38. In May 2008, Tiversa targeted LabMD as a potential customer. Tiversa contacted LabMD to inform it that it had obtained a copy of a LabMD file, allegedly on a P2P network. This particular file was a 1,718-page PDF document containing Personal Information on approximately 9,300 patients (the "1718 File"). The 1718 File was a victim of inadvertent file sharing.

39. In truth, Tiversa had, without any authority, accessed and downloaded ("hacked")[3] the 1718 File directly from a LabMD billing computer in Atlanta, Georgia on

[3] According to Black's Law Dictionary (10th Edition) "hack" means "to surreptitiously break into the computer, network, or database of another person or organization." A "hacker" is defined as "someone who surreptitiously uses or changes the information in another's computer system."

February 25, 2008. Tiversa's unauthorized download and retention of the 1718 File was a violation of several state and federal crimes.

40. LabMD would not learn that Tiversa had downloaded the 1718 File directly from a LabMD computer in Atlanta, Georgia, and nowhere else, before Richard E. Wallace revealed this fact to LabMD's chief executive office, Michael J. Daugherty, on April 2, 2014.

41. The filename on the document Tiversa hacked was "insuranceaging_6.05.071.pdf". The chance that anyone would ever have searched for or found the 1718 file was extremely remote. In order for a normal user on a P2P network to receive a search result for the "insuranceaging_6.05.071.pdf" file, that person would have to have searched for the document using the highly unusual search terms "insuranceaging" or "6.05.071".

42. On or about April 18, 2008, Tiversa sent CIGNA, a Tiversa customer, a report stating that Tiversa had found the 1718 File on a LabMD computer in Atlanta, Georgia with an IP address of 64.190.82.42 on April 18, 2008. The date was false but Tiversa's admission that it acquired the 1718 file directly from a LabMD computer was true and correct.

43. LabMD would not learn about the April 18, 2008 report to CIGNA until several days before the May 5, 2015 trial testimony of Richard Wallace[4] in *In re LabMD, Inc.*, in the United States Federal Trade Commission, Docket No. 9357 (the "Enforcement Action"). The April 18, 2008 report to CIGNA would have exculpated LabMD.

Tiversa Defrauds LabMD

44. On May 13, 2008, Tiversa and Boback falsely and fraudulently reported to Alison Simmons and John Boyle at LabMD that Tiversa had detected and downloaded the 1718 File from a "P2P network," when, in fact, Tiversa had hacked directly into a LabMD computer in

[4] The trial testimony of Richard E. Wallace ("Wallace Testimony") is in the record at ECF No. 63-2, beginning on p. 10. The Wallace Testimony is incorporated herein by reference.

Atlanta, Georgia, to capture and download the 1718 File into Tiversa's database with no authority or permission from anyone (False Statement No. 1[5]).

45. LabMD would not learn that Tiversa had downloaded the 1718 File directly from a LabMD computer in Atlanta, Georgia, and nowhere else, before Richard E. Wallace revealed this fact to LabMD's chief executive office, Michael J. Daugherty, on April 2, 2014.

46. On May 13, 2008, Tiversa and Boback falsely reported to Alison Simmons and John Boyle at LabMD that Boback did not know when or where Tiversa had obtained the 1718 File (False Statement No. 2).

47. LabMD would not learn that Tiversa knew exactly where it obtained and when it took the 1718 File before Richard E. Wallace revealed these facts to LabMD's chief executive office, Michael J. Daugherty, on April 2, 2014.

48. On May 13, 2008, Tiversa and Boback sent a fraudulent email to John Boyle at LabMD. The fraudulent email purported to be from Rick Wallace to "Mr. Boback" but, in fact, was not authored by Mr. Wallace. The email falsely claimed that:

- Tiversa's records showed that the 1718 File was continually available on peer-to-peer networks for sporadic periods over the past several months;
- Tiversa's computer system did not auto-record the IP;
- Even if the actual source IP address was in Tiversa's files, it was not readily available and it would take Tiversa "some time" to locate the information.

(Collectively, False Statement No. 3).

[5] LabMD's numbering of Tiversa's frauds and defamatory statements is solely for reference. The numbers are not meant to indicate order, hierarchy or any limitation on or actual count of all of the fraudulent and defamatory statements made by Defendants.

49. LabMD would not learn before Richard E. Wallace revealed the facts to LabMD's chief executive officer, Michael J. Daugherty, on April 2, 2014 that (1) Tiversa always knew that the 1718 File had never been continually available on peer-to-peer networks at any time, (2) Tiversa's computer system did auto-record the IP and (3) the source IP address was always readily available to Tiversa.

50. In an email dated May 22, 2008 from Boback to John Boyle at LabMD, Boback and Tiversa falsely represented to LabMD that:

- Tiversa "continued to see people searching for the file in question on the P2P network;"
- People were "searching precisely for the exact file name of the file in question;" and
- People "may or may not have been successful in downloading the file…."

(Collectively, False Statement No. 4).

51. LabMD would not learn before Richard E. Wallace revealed the facts to LabMD's chief executive office, Michael J. Daugherty, on April 2, 2014 that (1) Tiversa never saw anyone searching for the 1718 File other than LabMD, (2) no one, other than LabMD, ever searched for the 1718 by its precise filename, (3) other than Tiversa, no one had been successful in downloading the 1718 File.

52. In another email on May 22, 2008, Boback and Tiversa falsely represented to LabMD that it needed "to act quickly to avoid further spread." (False Statement No. 5). Boback and Tiversa knew that neither the 1718 File nor any other LabMD files had proliferated or "spread" to other computers on peer-to-peer networks or otherwise.

53. LabMD would not learn before Richard E. Wallace revealed the fact to LabMD's chief executive office, Michael J. Daugherty, on April 2, 2014 that the 1718 File had never proliferated or spread to other computers on peer-to-peer networks or otherwise.

54. In an email dated June 6, 2008, Boback and Tiversa falsely represented to LabMD that the 1718 File "will most likely have been already taken by secondary disclosure points which will need to be found and remediated" (False Statement No. 6).

55. LabMD would not learn before Richard E. Wallace revealed the fact to LabMD's chief executive office, Michael J. Daugherty, on April 2, 2014 that the 1718 File had never been taken by secondary disclosure points.

56. In an email dated July 15, 2008, Boback and Tiversa falsely represented to LabMD that:

- "We have continued to see individuals searching for and downloading copies of the file that was provided;" and

- "43 of the 50 states have very strict laws requiring the immediate notification of the affected individuals. It is very important that you contact the individuals affected asap."

(Collectively, False Statement No. 7).

57. LabMD would not learn before Richard E. Wallace revealed the fact to LabMD's chief executive office, Michael J. Daugherty, on April 2, 2014 that the 1718 File had never been downloaded by anyone other than Tiversa.

58. On November 21, 2008, counsel for LabMD received a telephone call from Jim Cook of the Cook Law Group in Pittsburgh, PA, on behalf of Tiversa. Through Cook, Tiversa falsely represented that the 1718 File had been leaked from LabMD into the public domain. Cook implied that Tiversa was in discussions about the 1718 File and stated, falsely, that Boback

and Tiversa were concerned that if they did not disclose the "leak" to the FTC, they may be sued for having knowledge of the "breach" and not reporting it (False Statement No. 8).

59. LabMD would not learn before Richard E. Wallace revealed the fact to LabMD's chief executive office, Michael J. Daugherty, on April 2, 2014 that the 1718 File had never leaked anywhere, much less the public domain.

60. Tiversa and Boback made misrepresentations to LabMD for the purpose of soliciting its business, specifically to try to persuade LabMD to use Tiversa's "Incidence Response Services."

61. LabMD refused Tiversa's solicitations, but in good faith reliance on Boback and Tiversa's False Statements, LabMD spent thousands of dollars and devoted hundreds of man-hours to seek to detect and remedy what was, in truth, a phantom data breach.

62. Tiversa and Boback knew about LabMD's investigation and knew that such an investigation was not necessary because Tiversa and Boback knew that on February 25, 2008, a Tiversa employee, while using a stand-alone computer:

- hacked directly into a LabMD computer in Atlanta, Georgia;
- targeted and took control of software on that computer;
- targeted the 1718 File located in a file on that computer;
- targeted and utilized the "push" feature of software on LabMD's computer to capture and push the 1718 File through LabMD's firewall in Atlanta, Georgia[6] to Tiversa's computer in Pittsburgh, Pennsylvania;

[6] The push feature of filesharing software is discussed on pp. 72 of "Filesharing Programs and 'Technological Features to Induce Users to Share,'" A Report to the United States Patent and Trademark Office from the Office of International Relations, Prepared by Thomas D. Sydnor II, John Knight and Lee A. Hollaar (November 2006). As of January 27, 2016, this paper was available for download at www.uspto.gov/ip/global/copyrights/cpright_filesharing_v1012.pdf.

- targeted and utilized the "browse host" feature of the software on LabMD's computer to learn that 18 other files could be taken from that computer;

- targeted, captured and then pushed those 18 files through LabMD's firewall to Tiversa's computer in Pittsburgh; and

- confirmed from a review of the 19 files that the owner of the files was LabMD and that LabMD was located in Atlanta, Georgia.

63. Tiversa and Boback have always known that they never found the 1718 File anywhere other than on a LabMD computer in Atlanta, Georgia. Yet by continuing to lie to LabMD, Tiversa and Boback caused LabMD to suffer unnecessary harm. LabMD would not have undertaken such an investigation if Tiversa and Boback had not lied to LabMD.

64. Boback and Tiversa knew that each of their False Statements were material misrepresentations of fact.

65. Boback and Tiversa made each of the False Statements with knowledge of their falsity or were reckless as to whether they were true or false.

66. Boback and Tiversa intended for LabMD to rely upon those statements by incurring enough costs in their own investigation that they would eventually be motivated to hire Tiversa after LabMD failed to uncover the truth.

67. Boback and Tiversa's allegations were very serious to LabMD. LabMD justifiably relied on these misrepresentations by conducting an unnecessary investigation at a great cost to LabMD of time and money.

Tiversa Lies to Cigna

68. In a Forensic Investigation Report prepared by Tiversa and sent to CIGNA on or about August 12, 2008, Tiversa falsely reported to CIGNA that:

- Tiversa had observed the 1718 File at IP addresses other than the IP address for LabMD (including 68.8.250.203 which, Tiversa told CIGNA resolved to the IP address of a known identity thief in San Diego, CA);

- Tiversa had observed other of LabMD's files at IP addresses other than the IP address for LabMD;

- Network constraints and/or user behavior prevented Tiversa from downloading any of LabMD's files from the other IP addresses;

- LabMD files, including the 1718 File, had proliferated across peer-to-peer networks and were available for downloading from additional IP addresses;

- Users had logged off the peer-to-peer network prior to or while Tiversa was attempting to acquire LabMD's files from other IP addresses; and

- Tiversa recommended that CIGNA and/or LabMD investigate the data (falsely implying to CIGNA that LabMD had not and was not investigating).

69. Tiversa would later submit this false report to the FTC for use in the Enforcement Action as evidence to support its lies. The falsified report to CIGNA (and later attempt to rely upon that report) was part of Tiversa's concealment of its lies to LabMD and others.

70. LabMD would not learn about the August 12, 2008 report to CIGNA until several days before the May 5, 2015 trial testimony of Richard Wallace in the Enforcement Action.

71. Boback and Tiversa knew that LabMD was a small cancer-testing laboratory providing doctors with cancer-detection services.

72. Boback and Tiversa knew that LabMD's success depended upon the confidence of its employees, patients, providers, third party payors, insurance carriers and referral sources,

that LabMD would keep patients' personal health information ("PHI") and personal identifying information ("PII") confidential.

73. Boback and Tiversa knew that if they, directly or indirectly, represented to any of LabMD's employees, patients, providers, third party payors, insurance carriers and referral sources that LabMD had failed to keep PHI and PII confidential, that such representations would erode if not eradicate the confidence that employees, patients, providers, third party payors, insurance carriers and referral sources had in LabMD.

74. Boback and Tiversa knew that false, fraudulent and defamatory representations that LabMD had made patients' PII and PHI publicly available or otherwise disclosed that information on P2P networks (collectively, "Defamatory Statements Regarding Disclosure") were allegations of business misconduct that would cause harm to LabMD's reputation so as to lower it in the estimation of the employees, patients, providers, third party payors, insurance carriers, referral sources and other communities and would deter employees, patients, providers, third party payors, insurance carriers, referral sources and others from associating or dealing with it. Boback and Tiversa knew that these false representations would instill in the minds of others an impression that would adversely affect LabMD's fitness for the proper conduct of its lawful business. False representations about LabMD's abilities to keep PII and PHI confidential were particularly harmful to LabMD due to legal, ethical and other of the company's duties to maintain such information in confidence.

75. Boback and Tiversa knew that false, fraudulent and defamatory representations that LabMD's 1718 File was found somewhere other than on a LabMD computer ("Defamatory Statements Regarding Source") were allegations of business misconduct that would cause harm to LabMD's reputation so as to lower it in the estimation of the employees, patients, providers,

third party payors, insurance carriers, referral sources and other communities and would deter employees, patients, providers, third party payors, insurance carriers, referral sources and others from associating or dealing with it. Boback and Tiversa knew that these false representations would instill in the minds of others an impression that would adversely affect LabMD's fitness for the proper conduct of its lawful business. False representations about LabMD's abilities to keep PII and PHI confidential were particularly harmful to LabMD due to legal, ethical and other of the company's duties to maintain such information in confidence.

76. Boback and Tiversa knew that false, fraudulent and defamatory representations that LabMD's 1718 File had proliferated to multiple places on peer-to-peer networks ("Defamatory Statements Regarding Spread") were allegations of business misconduct that would cause harm to LabMD's reputation so as to lower it in the estimation of the employees, patients, providers, third party payors, insurance carriers, referral sources and others and would deter employees, patients, providers, third party payors, insurance carriers, referral sources and others from associating or dealing with it. Boback and Tiversa knew that these false representations would instill in the minds of others an impression that would adversely affect LabMD's fitness for the proper conduct of its lawful business. False representations about LabMD's abilities to keep PII and PHI confidential were particularly harmful to LabMD due to legal, ethical and other of the company's duties to maintain such information in confidence.

77. Defamatory Statements Regarding Disclosure, Defamatory Statements Regarding Source and Defamatory Statements Regarding Spread will hereinafter collectively be referred to as "Defamatory Statements Regarding Disclosure, Source and Spread."

Tiversa Defrauds FTC Investigators and Defames LabMD

78. Tiversa and certain staff members of the Federal Trade Commission began working together in 2007 on the topic of inadvertent file sharing on P2P networks.

79. Boback believed Tiversa could capitalize on its newfound arrangement with the FTC by reporting to the FTC companies that refused Tiversa's services, the expected result of which was that (1) those companies would respond to FTC inquiries by hiring Tiversa and/or (2) Tiversa would exact revenge on those companies for not hiring Tiversa in the first place.

80. The FTC intended to capitalize on its relationship with Tiversa by using Tiversa's technological capabilities and expertise to identify targets for investigations and prosecutions and by using evidence obtained from Tiversa to prosecute.

81. In late 2007 or early 2008, members of the FTC staff visited Boback at Tiversa's facility in Pennsylvania. Following that meeting, the FTC began requesting that Tiversa provide information to the FTC.

82. Throughout 2008 and 2009, Tiversa collected information on companies that, it would later claim, had allowed personal identifying information (PII) and personal health information (PHI) to become "available" on peer-to-peer networks. Tiversa compiled a list of approximately 90 of such companies to give to the FTC (the "List") in furtherance of its partnership with the FTC.

83. When Boback learned that Mike Daugherty at LabMD ultimately refused to do business with Tiversa, Boback said to one of Tiversa's analysts, "f--- him, make sure he's at the top of the [L]ist."[7]

[7] See Wallace Testimony at ECF No. 63-2, p. 17.

84. In 2009, Tiversa made numerous false, fraudulent and defamatory statements to FTC investigators about LabMD including Defamatory Statements Regarding Disclosure, Source and Spread which included statements to the following effect:

- LabMD had publicly disclosed patients' PII and PHI (Defamatory Statement No. 1);
- LabMD's 1718 File was found somewhere other than on a LabMD computer (Defamatory Statement No. 2); and
- LabMD's 1718 File had proliferated to multiple places on peer-to-peer networks (Defamatory Statement No. 3).

85. The Defamatory Statements Regarding Disclosure, Source and Spread (including, without limitation, Defamatory Statement Nos. 1, 2 and 3) were false and defamatory, were known by Boback and Tiversa to be false and defamatory, were understood by recipients of the statements to apply to LabMD, were intended to harm LabMD and did, in fact, cause special harm LabMD.

86. LabMD would not learn that Tiversa and Boback had made the Defamatory Statements Regarding Disclosure, Source and Spread to the FTC at any time and that Tiversa and Boback's Statements Regarding Disclosure, Source and Spread were false until after Richard E. Wallace revealed these facts to LabMD's chief executive officer, Michael J. Daugherty, on April 2, 2014.

87. In 2009, FTC investigators felt they needed to serve a civil investigative demand on Tiversa to formally obtain the List and other documentation to investigate and prosecute LabMD and other companies. Tiversa, however, was concerned about public disclosure of this aspect of its relationship with the FTC.

88. To resolve Tiversa's dilemma, Tiversa, Boback, FTC investigators and Tiversa's counsel agreed that (1) Tiversa would create a shell company (later named "The Privacy Institute"), (2) the FTC investigators would serve a civil investigative demand on that company rather than on Tiversa and (3) Tiversa would produce the List and other documents to the FTC investigators under the pretense that those items were being produced by The Privacy Institute.

89. In 2009, Tiversa directed its counsel at Morgan Lewis to incorporate The Privacy Institute as a Delaware corporation.

90. The Privacy Institute was created to avoid any connection with Tiversa. Shortly after its creation, FTC investigators followed through on the plan to serve a civil investigative demand on The Privacy Institute. In response, Tiversa produced the List and other documents to the FTC investigators.

91. Tiversa knew that The Privacy Institute was a sham and that the use of this sham organization would allow Tiversa to produce whatever it wanted and to withhold whatever it wanted. By doing so, Tiversa could withhold any evidence that would exculpate LabMD or otherwise prove that the Statements Regarding Disclosure, Source and Spread were false, fraudulent and defamatory.

92. Tiversa's creation and use of The Privacy Institute as a conduit to the FTC was a further effort to conceal it and Boback's frauds, falsities and defamation. Tiversa and Boback did not care whether Tiversa's "evidence" was false, fraudulent, defamatory or otherwise. The point was to instigate the FTC to investigate LabMD and other companies to (1) increase the chance that LabMD and the other companies would hire Tiversa and (2) to exact revenge on those companies that refused to hire Tiversa.

93. Tiversa included LabMD and its 1718 File on the List in retaliation for LabMD's refusal to purchase Tiversa's services.

94. LabMD would not learn about the existence of the List (but not its contents) until the November 21, 2013 deposition of Boback in the FTC Enforcement Action.

95. LabMD would not learn about the contents of the List until after it was produced by Richard E. Wallace just a few days before his testimony in the Enforcement Action on May 5, 2015.

96. Tiversa made Defamatory Statements Regarding Disclosure, Source and Spread to the FTC investigators in the fall of 2009 when Boback and others at Tiversa met them in Washington, D.C. to discuss Tiversa's response to the civil investigative demand served on The Privacy Institute. On information and belief, the FTC Staff expressed concerns that they needed more and better evidence for its investigations.

97. On the return trip from their meeting with the FTC, Boback told Wallace that Tiversa needed to increase the apparent "spread" of the files identified on the List. Wallace was to search for the files again to see if they were available at IP addresses in addition to the address in Tiversa's database, and that if the files were not, in fact, available at any additional IP addresses, Wallace was told to create or alter data in Tiversa's database to make it appear that the files were available at additional IP addresses.

98. The Defamatory Statements Regarding Disclosure, Source and Spread caused the FTC to investigate LabMD. In fact, the FTC investigators adopted Tiversa's fraud and relied upon Tiversa's Defamatory Statements Regarding Disclosure, Source and Spread. An example of the FTC investigators' use of and reliance on Tiversa's Defamatory Statements Regarding Disclosure, Source and Spread is seen in the following sentence in an FTC investigator's January

19, 2010 letter to LabMD (almost a year and a half *after* LabMD addressed the alleged disclosure problem by removing the offending software from its computer):

> According to information we have received, a computer file (or files) from your computer network *is* available to users on a peer-to-peer file sharing ("P2P") network (hereinafter, "P2P breach").

(Emphasis added.)

99. LabMD was not able to refute the FTC investigators allegations until after Richard E. Wallace began to dispel the frauds in his conversation with LabMD's chief executive officer, Michael J. Daugherty, on April 2, 2014.

100. The FTC's investigation of LabMD evolved into an enforcement action against the company for alleged failure to reasonably protect the security of consumers' personal data, including medical information. The FTC would not have investigated LabMD, and certainly would not have commenced an enforcement action against it, but for the Defamatory Statements Regarding Disclosure, Source and Spread and Defendants' willingness to support the FTC investigators with false, fraudulent and defamatory evidence.

101. LabMD was kept in the dark about the Defamatory Statements Regarding Disclosure, Source and Spread. At no time during their investigation did the FTC investigators disclose to LabMD what evidence they were relying upon as a basis for investigating LabMD.[8] LabMD tried to learn how Tiversa and the FTC came to possess the 1718 File and what

[8] On November 20, 2015, Michael J. Daugherty and LabMD filed a Bivens action against the FTC Investigators in Washington, D.C. See *Michael J. Daugherty and LabMD, Inc. v. Alain H. Sheer, Ruth T. Yodaiken and Carl H. Settlemyer, III*, in the United States District Court for the District of Columbia, Civil Action No. 1:15-cv-02034. As alleged therein, the FTC Investigators were or became complicit in Tiversa's fraud. The timing, extent and circumstances of their complicity is expected to develop in discovery.

information Tiversa had provided to the FTC investigators but the investigators refused to provide answers.

102. By letter dated September 30, 2010, LabMD asked Tiversa to explain how it came to possess the 1718 File. Like the FTC investigators, Tiversa kept LabMD in the dark. In a further effort to conceal its fraud, falsities and defamation, Tiversa refused to provide LabMD with any information at all.

103. LabMD would not learn how Tiversa came to possess the 1718 File before Richard E. Wallace explained to LabMD's chief executive officer, Michael J. Daugherty, on April 2, 2014, that Tiversa obtained the 1718 File directly from a LabMD computer in Atlanta, Georgia and that the 1718 File had never been found anywhere else.

104. In or about October 2013, shortly after *The Devil Inside the Beltway* was published, Tiversa gave to the FTC a document that would later be relied upon by the FTC as evidence of LabMD's alleged wrongdoing. The FTC introduced CX00019 at the trial of the Enforcement Action.

105. CX00019 contains four IP addresses where Tiversa supposedly found the 1718 File on P2P networks. (False Statement No. 9, Defamatory Statement No. 4.) In truth, Tiversa never found the 1718 File at any of the IP locations on CX00019. This document was another intentional fabrication of evidence, another effort by Tiversa to conceal the fact that it had been providing false, fraudulent and defamatory information to the FTC ever since 2009 and further evidence of Tiversa and Boback's retaliation against LabMD.

106. LabMD would not learn that the four IP addresses in CX00019 were fabricated until after Richard E. Wallace disclosed the truth to LabMD's chief executive officer, Michael J. Daugherty, on April 2, 2014.

Tiversa and Boback Commit Fraud on the Court in the
Georgia Action to Conceal Their Frauds, Falsities and Defamation

107. On October 19, 2011, LabMD sued Tiversa in the Superior Court of Fulton County (the "Georgia Action") on a number of claims. LabMD anticipated that it would learn through discovery how Tiversa came to possess the 1718 File and what information Tiversa had provided to the FTC Investigators. The FTC and Tiversa had kept LabMD in the dark and LabMD needed discovery to get answers. In a further effort to conceal their frauds, falsities and defamation, Tiversa and Boback committed fraud on the court to escape jurisdiction in Georgia in order to avoid formal discovery that was likely to lead to exposure of Tiversa's and Boback's frauds, falsities and defamation.

108. The Georgia Action was removed to the United States District Court for the Northern District of Georgia on November 21, 2011.

109. On November 30, 2011, Tiversa moved to dismiss all claims against it for, *inter alia*, lack of personal jurisdiction (the "Motion to Dismiss").

110. On August 15, 2012, the district court granted Tiversa's Motion to Dismiss, finding that the Court lacked personal jurisdiction over Tiversa.

111. On February 5, 2013, the Eleventh Circuit affirmed the trial court's grant of Tiversa's Motion to Dismiss, finding that the Court lacked personal jurisdiction over Tiversa. *LabMD, Inc. v. Tiversa, Inc.*, 509 Fed. Appx. 842 (11th Cir. 2013).

112. On January 29, 2016, LabMD filed its Rule 60(d)(3) Motion for Relief from Judgment in the Georgia Action.[9]

[9] *See* ECF Nos. 33 and33-1 in *LabMD, Inc. v. Tiversa, Inc., Trustees of Dartmouth College and M. Eric Johnson*, in the United States for the Northern District of Georgia, Civil Action No. 1:11-cv-0404-LMM. That motion and the accompanying brief in support are incorporated herein by reference.

113. LabMD's Rule 60(d)(3) motion is based largely on its discovery that Tiversa committed numerous frauds on the court, including the following misrepresentation from its briefs before the district court and the Eleventh Circuit:

114. In support of Tiversa's Motion to Dismiss, Boback falsely declared that "Tiversa does not regularly solicit business in Georgia" (Fraud Statement No. 1) and "Neither Tiversa nor any of its employees or agents have ever conducted any business in Georgia, engaged in a persistent course of conduct in Georgia or derived any revenue from the rendition of services in Georgia, and particularly in any way related to the allegations of LabMD, Inc. ("LabMD") in the Complaint."[10] (Fraud Statement No. 2).

115. The following statements made by Tiversa in its briefing are also false and were known to be false at the time they were made:

- "Here, it is undisputed that Tiversa did not hack any computers, did not somehow target LabMD or even know where LabMD and its servers were located when it downloaded the 1,718 File." (Fraud Statement No. 3).

- "As set forth in Tiversa's prior brief and the accompanying Boback Declaration, Tiversa's only solicitation of business to date in the state of Georgia consists of the one phone call and eight emails to LabMD described in the Complaint. These nine contacts to one potential customer over a two month period over two and half years ago cannot reasonably be deemed regular solicitation of business in the state of Georgia." (Fraud Statement No. 4).

- "Tiversa's only contact with Georgia is one phone call and eight emails placed to LabMD during the period of May through July 2008." (Fraud Statement No. 5).

- "Tiversa has no customers and conducts no business in Georgia, and its only effort ever to solicit business in Georgia – consisting of one phone call and eight emails to

[10] See Paragraph Nos. 10 and 15 of the Boback Declaration at ECF No. 8-1 in the Georgia Action.

LabMD during a two-month period over four years ago – does not constitute "regularly" soliciting business." (Fraud Statement No. 6).

- "Tiversa did not target or direct its activities at the State of Georgia. Instead, it downloaded a publicly available file from a P2P file sharing network without knowledge of the file's location." (Fraud Statement No. 8).

- "In this case, Tiversa did not do or fail to do anything within the State of Georgia." (Fraud Statement No. 9).

116. The district court and the Eleventh Circuit relied upon Boback's Declaration to conclude that Tiversa's one phone call and handful of emails to LabMD was not sufficient under Georgia law to subject Tiversa to personal jurisdiction in Georgia courts. *LabMD, Inc. v. Tiversa, Inc*., 509 Fed. Appx. 842, 845 (11th Cir. 2013).

117. In truth, Tiversa had solicited at least five (5) other companies in Georgia during the same time it was soliciting LabMD. These facts are evident from the List Tiversa secretly gave to the FTC Investigators.

118. Neither Tiversa nor the FTC would *ever* give LabMD a copy of the List. As noted above, LabMD would not learn about the *existence* of the List (but not its contents) until the November 21, 2013 deposition of Boback in the FTC Enforcement Action. LabMD would not learn about the *contents* of the List until it was produced by Richard E. Wallace just a few days before his testimony in the Enforcement Action on May 5, 2015.

119. The List establishes that Boback's sworn declarations and Tiversa's representations in the Georgia Action were knowingly false.

120. Tiversa committed fraud on the court in the Georgia Action to prevent LabMD from discovering that Tiversa had made Defamatory Statements Regarding Disclosure, Source

and Spread to the FTC investigators and to prevent LabMD from proving that the FTC was relying upon false, fraudulent, defamatory and illegally obtained evidence.

121. In an effort to retaliate against LabMD and interfere with LabMD's pursuit of its rights, on September 5, 2013, almost a month before LabMD's October 6, 2013 deadline for filing a petition for certiorari in the Georgia Action, Tiversa and Boback sued LabMD and its chief executive officer Michael J. Daugherty for defamation in Pennsylvania in *Tiversa Holding Corp. and Robert J. Boback v. LabMD, Inc. and Michael J. Daugherty* in United States District Court for the Western District of Pennsylvania, Civil Action File No. 2:13-cv-01296 ("Tiversa's Federal Defamation Action").[11]

122. In yet another effort to retaliate and interfere with LabMD's pursuit of its rights, on September 23, 2014, during the pendency of Tiversa's Federal Defamation Action, Tiversa and Boback filed a state court defamation lawsuit against LabMD and Daugherty in Pennsylvania. See Praecipe for Writ of Summons in *Tiversa Holding Corp. and Robert J. Boback v. LabMD, Inc., Michael J. Daugherty and Cause of Action* [LabMD's law firm in the FTC Enforcement Action], in the Court of Common Pleas of Allegheny County, Pennsylvania, GD – 14-016497. ("Tiversa's State Defamation Action").

123. Tiversa successfully concealed its frauds from LabMD and others until long after the final judgment in the Georgia Action. As a consequence of Tiversa and Boback's concealment, LabMD did not learn the truth about the FTC's false, fabricated and defamatory evidence until Wallace contacted LabMD's chief executive officer and disclosed the truth on April 2, 2014.

[11] Mr. Daugherty's book, the subject of Tiversa and Boback's defamation claims, was not even published yet.

124. On May 5, 2015, Wallace testified to the following at trial in the Enforcement Action:

- On February 25, 2008, Wallace (as a Tiversa employee), using a stand-alone computer, located the 1718 File on a LabMD computer near Atlanta, Georgia.

- Wallace never found the 1718 File anywhere other than on a LabMD computer.

- At Boback's direction, Wallace and others would manipulate the data in Tiversa's data repositories to make it appear that prospective customers' files had spread to other locations on the peer-to-peer networks.

- Tiversa would never tell prospective customers where their files were found. Tiversa would claim that the IP addresses of the source computers were not recorded. Wallace said this was a lie – Tiversa always knew the IP addresses of the source computers.

125. Wallace further testified that before Boback's deposition on November 21, 2013, Boback told Wallace to change data in Tiversa's data store to make sure that the 1718 File did not appear to have come from the Atlanta area. This is yet another example of Tiversa's efforts to conceal its frauds, falsities and defamation.

126. Tiversa terminated Wallace's employment shortly after Wallace's deposition was noticed in the Enforcement Action in early 2014. Wallace was terminated after he told Boback that he would not lie under oath. Tiversa's termination of Wallace was another effort by Boback and Tiversa to conceal the truth.

Other Concealment

127. On February 25, 2009, Tiversa alleged to the public at large that it had found that an Iranian computer was in possession of blueprints for the cockpit of Marine One, the

President's helicopter. According to Tiversa, the Iranian computer disclosed the document on a P2P network between October 27, 2006, and February 25, 2009.

128. Beginning in 2014, the House Oversight Committee had great doubts about the veracity of Tiversa's Marine One story. *See* Staff of H. Comm. on Oversight and Government Reform, 113th Cong., Tiversa, Inc.: White Knight or Hi-Tech Protection Racket? (2015)[12] (hereinafter the "OGR Report"), at p. 17. Those doubts were fueled by the fact that Tim Hall, the NCIS employee who investigated the Marine One leak several years earlier, is now the Director of Government Services at Tiversa. OGR Report at 17. Tiversa hired Hall before he completed his investigation.

129. LabMD would not learn about Tiversa's hiring of the NCIS investigator until the ORG Report was published after Wallace's May 5, 2015 testimony.

130. Tiversa's hiring of the NCIS investigator is an example of the lengths to which Boback and Tiversa will go to conceal the truth. If Tiversa had not interfered with the NCIS investigation by hiring the investigator, the investigation would have exposed Tiversa as a fraud, the FTC would not have continued to rely on Tiversa's fictionalized evidence, the FTC would have stopped its investigation and the FTC would never have filed the Enforcement Action.

More of Tiversa and Boback's Defamatory Statements

131. The following statements published by Tiversa and Boback in Tiversa's May 28, 2009 press release (RICO Case Statement at 13, Ex. G) about LabMD, are false and defamatory, were known by Boback and Tiversa to be false and defamatory, were understood by recipients of the statements to apply to LabMD, were intended to harm LabMD and did, in fact, cause special harm LabMD:

[12] A true and correct copy of the OGR Report is in the record in this case beginning on p. 2 of ECF No. 63-1. The OGR Report is incorporated herein.

- Tiversa today announced the findings of new research that revealed 13,185,252 breached files emanating from over 4,310,839 sources on P2P filesharing networks within a twelve month period from March 01, 2008 - March 01, 2009. (Defamatory Statement No. 5).

- This new data clearly demonstrates that P2P file-sharing risk is not effectively being addressed by the security protocols of Fortune 500 companies and government agencies, as these organizations commonly have exposure across the Extended Enterprise. (Defamatory Statement No. 6).

- Findings released in February 2009, in a collaborative research study ("Data Hemorrhages in the Health-Care Sector") between Tiversa and The Tuck School of Business at Dartmouth College highlight these same risks by focusing on the exposure rate of sensitive data in the healthcare industry. (Defamatory Statement No. 7).

- Over a two-week period, Dartmouth College researchers and Tiversa searched file-sharing networks for key terms associated with the top ten publicly traded health care firms in the country, and discovered a treasure trove of sensitive documents. (Defamatory Statement No. 8).

- Also identified was a 1,718-page document from a medical testing laboratory containing patient Social Security numbers, insurance information, and treatment codes for thousands of patients….(Defamatory Statement No. 9).

132. Defamatory Statement Nos. 5-9 are expressly and/or impliedly false because LabMD never experienced a security breach. The 1718 File was not a breached file, it was a stolen file. LabMD was effectively addressing security. LabMD did not have exposure across the Extended Enterprise. Dartmouth and Tiversa did not discover a "treasure trove" of sensitive documents. In the case of the 1718 File, Tiversa hacked into a LabMD computer and took that file without any authorization or permission. Tiversa committed state and federal crimes by hacking into a LabMD computer and taking what it had no right to take.

133. LabMD could not disprove Tiversa and Boback's Defamatory Statements in Tiversa's press release until after Richard E. Wallace revealed the truth to LabMD's chief executive officer, Michael J. Daugherty, on April 2, 2014.

134. The following statements published by Tiversa and Boback in their February 10, 2015 statement to "The Pathology Blawg" (RICO Case Statement at 9-10, Ex. E) are false and defamatory, were known by Boback and Tiversa to be false and defamatory, were understood by recipients of the statements to apply to LabMD, were intended to harm LabMD and did, in fact, cause special harm LabMD:

- After all, we found this file in a public file sharing network that was accessible by millions of people from around the world. (Defamatory Statement No. 10).

- The FTC then filed a Civil Investigative Demand (CID) that forced Tiversa to comply. In compliance with the CID, Tiversa provided information on 84 companies that were breaching information and that matched the criteria of the CID. LabMD was one of those listed. (Defamatory Statement No. 11).

- Tiversa has not had a single criminal allegation alleged against us by any individual or organization in our entire 11 year history…..not even Daugherty or LabMD, despite the defamatory and baseless allegations of extortion, theft and fraud. One would think that if Daugherty truly believed he was the victim of an actual extortion plot, as he has suggested, he would have called the police or FBI. To my knowledge, he has not. It is my belief that he knows that if he files a false police statement, he could be prosecuted, which may be the likely reason why he has decided not to do so. (Defamatory Statement No. 12).

- LabMD lawsuit – The claims are baseless and completely unsubstantiated….even in the complaint itself. This appears to be another attempt by Daugherty to distract people from the INDISPUTABLE FACT that LabMD and Michael Daugherty leaked customer information on nearly 10,000 patients. (Defamatory Statement No. 13).

- To my understanding from the deposition transcripts, LabMD had a policy against installing file sharing software. An employee at LabMD violated that policy, which resulted in the exposure of nearly 10,000 patients private information. This clearly demonstrates that LabMD DID NOT adequately protect their patient's PHI/PII, which

> is al that the FTC needs to demonstrate. Case closed. The rest of this is just a desperate attempt to distract everyone from that INDISPUTABLE FACT. (Defamatory Statement No. 14).

135. Defamatory Statement Nos. 10-14 are expressly and/or impliedly false because the 1718 File was not found in "a public file sharing network that was accessible by millions of people from around the world." The FTC did not file or serve a civil investigative demand on Tiversa. Tiversa was not forced to provide any information on any companies. LabMD did not breach any information to anyone. As noted above, the FTC investigators served their civil investigative demand on The Privacy Institute, not Tiversa. The purpose of this sham organization was to conceal Tiversa and Boback's fraud and to give Tiversa the ability to produce and withhold whatever it and Boback wanted. Although LabMD's name was not mentioned in the civil investigative demand, Tiversa, Boback and the FTC investigators had already discussed LabMD. Everyone knew that LabMD's name would be on the List. Other companies had the same or similar outcomes as LabMD, including, without limitation, Franklin's Budget Auto Sales, Inc. Tiversa's taking of the 1718 File and other documents was a violation of state and federal crimes. Daugherty did not avoid any law enforcement agency for fear of the consequences of filing a false report. Neither LabMD nor Mike Daugherty ever attempted to divert "everyone" from the FTC's allegations. The FTC's allegations were based on fictionalized evidence provided by Tiversa, not "indisputable facts."

136. The following statements made by Boback and Tiversa in a letter to the editor of the Wall Street Journal, published in the December 9, 2015 edition of the Journal, are false and defamatory, were known by Boback and Tiversa to be false and defamatory, were understood by recipients of the statements to apply to LabMD, were intended to harm LabMD and did, in fact, cause special harm LabMD:

- LabMD, a Georgia-based cancer screening company, admits its own employee mistakenly exposed the confidential medical records of nearly 10,000 individuals on the Internet. (Defamatory Statement No. 15).

- LabMD's CEO Michael Daugherty admits that a LabMD employee improperly installed LimeWire file-sharing software on a company computer. Doing so made confidential patient information publicly available over the Internet. (Defamatory Statement No. 16).

- Using this information, LabMD discovered that it had peer-to-peer sharing software on a company computer. Without Tiversa's free information, LabMD would have never known it was continuing to publicly expose patient information. (Defamatory Statement No. 17).

- The suggestion that Tiversa provided information on exposed files to the Federal Trade Commission as a means of retribution because LabMD didn't hire Tiversa is 100% false. (Defamatory Statement No. 18).

- In the Fall of 2009—well over a year later—as part of its investigation into cyber leaks, the FTC issued the equivalent of a subpoena to Tiversa, which legally required us to provide information on all the breaches we found from many companies. There was absolutely no "deal" entered into between the FTC and Tiversa. It is no different than the subpoena the FTC issued on LabMD. LabMD was legally required to respond, as was Tiversa. (Defamatory Statement No. 19).

- As a result of this dispute, LabMD's CEO has defamed my company and made statements that are 100% wrong. (Defamatory Statement No. 20).

137. Defamatory Statement Nos. 15-20 are expressly and/or impliedly false because LabMD never admitted that any of its employees ever exposed anything on the Internet. An installation of LimeWire did not make confidential patient information publicly available over the Internet. Tiversa gave the FTC the 1718 File and other "evidence" in retribution for LabMD not hiring Tiversa. The FTC did not file or serve a civil investigative demand on Tiversa. Tiversa was not forced to provide any information on any companies. LabMD was not breaching information. LabMD did not match the criteria of the civil investigative demand. As noted above, the FTC investigators served their civil investigative demand on The Privacy Institute, not Tiversa. Tiversa was not legally required to produce anything or provide any

information. The purpose of this sham organization was to conceal Tiversa and Boback's fraud and to give Tiversa the ability to produce and withhold whatever it and Boback wanted. Tiversa did not comply with the civil investigative demand served on The Privacy Institute. Tiversa has profited from its partnership with the FTC. Although LabMD's name was not mentioned in the civil investigative demand, Tiversa, Boback and the FTC investigators had already discussed LabMD. Everyone knew that LabMD's name would be on the List. LabMD's chief executive officer has not defamed Boback or Tiversa. Tiversa acted illegally and inappropriately in all of its dealings with LabMD.

138. False Statements Regarding Disclosure, Source and Spread and Defamatory Statements Regarding Disclosure, Source and Spread are hereinafter collectively referred to as "False and Defamatory Statements Regarding Disclosure, Source and Spread."

139. Starting in 2008, Boback and Tiversa knew that LabMD was a small yet successful medical testing laboratory providing doctors with cancer-detection services.

140. Until Boback and Tiversa started making False and Defamatory Statements Regarding Disclosure, Source and Spread, LabMD was a trusted provider of services that had a reputation for honesty, integrity, respect for the confidentiality of PII and PHI and full compliance with all state and federal laws.

141. Boback and Tiversa knew that LabMD's success depended upon the confidence of its employees, patients, providers, third party payors, insurance carriers and referral sources that LabMD would keep patients' PII and PHI confidential.

142. Boback and Tiversa knew that if they, directly or indirectly, represented to any of LabMD's employees, patients, providers, third party payors, insurance carriers and referral sources that LabMD had failed to keep PHI and PII confidential, that such representations would

erode if not eradicate the confidence that employees, patients, providers, third party payors, insurance carriers and referral sources had in LabMD.

143. Boback and Tiversa knew its False and Defamatory Statements Regarding Disclosure, Source and Spread were allegations of business misconduct that would cause harm to LabMD's reputation so as to lower it in the estimation of the employees, patients, providers, third party payors, insurance carriers and referral sources other communities and would deter employees, patients, providers, third party payors, insurance carriers and referral sources and others from associating or dealing with it. Boback and Tiversa knew that these false representations would instill in the minds of others an impression that would adversely affect LabMD's fitness for the proper conduct of its lawful business. False representations about LabMD's abilities to keep PII and PHI confidential were particularly harmful to LabMD due to legal, ethical and other of the company's duties to maintain such information in confidence.

144. Boback and Tiversa knew that False and Defamatory Statements Regarding Disclosure, Source and Spread would capture the attention of government agencies, including the FTC, and that a government agency such as the FTC was likely to investigate and pursue an enforcement action against LabMD based on Tiversa's false evidence. Boback and Tiversa knew that if a government agency such as the FTC investigated or pursued an enforcement action against LabMD, that such efforts would be devastating to LabMD's reputation in the employees, patients, providers, third party payors, insurance carriers, referral sources and other communities and would deter employees, patients, providers, third party payors, insurance carriers, referral sources and others from associating or dealing with LabMD.

145. Boback and Tiversa intended for their False and Defamatory Statements Regarding Disclosure, Source and Spread to cause LabMD to suffer harm. Boback and Tiversa

targeted LabMD and wanted to make an example of LabMD to show other companies what would happen if they did not hire Tiversa or interfere with its objectives. Boback and Tiversa also wanted to punish LabMD for opposing the FTC in the Enforcement Action and for the publication of *The Devil Inside the Beltway*.

146. Boback and Tiversa's False and Defamatory Statements Regarding Disclosure, Source and Spread have been financially devastating to LabMD. The False Statements Regarding Disclosure, Source and Spread harmed LabMD by precipitating the FTC's investigation and enforcement action against it, based entirely on Tiversa's fabricated evidence. As a direct consequence of the FTC's proceedings, including the attendant adverse publicity and the administrative burdens that were imposed on LabMD to comply with the FTC's demands for access to current and former employees and the production of thousands of documents, LabMD's insurers cancelled insurance coverages for LabMD, and LabMD lost virtually all of its patients, referral sources, and workforce, which had included around 40 full-time employees. Consequently, LabMD was effectively forced out of business by January 2014, and it now operates as an insolvent entity that simply provides records to former patients.

147. Boback and Tiversa's False and Defamatory Statement Regarding Disclosure, Source and Spread caused LabMD to suffer reputational harm as well as actual damages, including the loss employees, patients, providers, third party payors, insurance carriers and referral sources, all of which resulted in a decline in LabMD's revenue and ultimately ruined LabMD's business.

148. Boback and Tiversa's False and Defamatory Statements Regarding Disclosure, Source and Spread tortiously interfered with LabMD's existing and prospective contracts with

employees, third party payors, and insurance carriers between May 2008 and LabMD's closure in January 2014.

149. The False and Defamatory Statements Regarding Disclosure, Source and Spread and other misconduct were done with the specific intent to harm LabMD's existing and prospective contractual relationships. Specifically, Boback and Tiversa wanted to put LabMD out of business (1) to prevent LabMD from learning and disclosing the truth behind their False and Defamatory Statements Regarding Disclosure, Source and Spread and (2) in retribution of the fact that LabMD did not hire Tiversa, that LabMD's chief executive officer published *The Devil Inside the Beltway* and that LabMD disclosed and challenged Tiversa and Boback's coercive business practices. Metaphorically speaking, Boback and Tiversa's method was to attack LabMD with a machine gun rather than one or two well-aimed bullets.

150. Boback and Tiversa were purposeful in their actions to destroy LabMD. For example, Boback and Tiversa planned and executed several maneuvers to cause LabMD to bleed to death before their frauds were revealed. Boback and Tiversa accomplished this with purposeful actions including, for example, causing LabMD to incur a devastating amount of attorneys' fees and litigation expenses. Specific examples of this include Tiversa and Boback's fraud on the court in the Georgia Action, the filing and frivolous pursuit of Tiversa's Federal Defamation Action and Tiversa's State Defamation Action and their continual provision of fabricated evidence and perjured testimony to the FTC. Boback and Tiversa also purposely acted, as discussed above, to injure LabMD's reputation to prevent employees, third party payors, insurance carriers and others from dealing with it.

151. Boback and Tiversa's tortious interference was aimed at existing employment relationships LabMD had with the following employees:

- Kindall R. Alvarez-Esquivel
- Dean'na Bagwell
- John Boyle
- Brandon Bradley
- Sandra C. Brown
- Anita S. Carson-Ford
- Mark M. Chaknis
- Thuhoa T. Dang
- Michael J. Daugherty
- Leah D. Devine
- Glenda M. Embleau
- Mary C. Fontaine
- Amanda Foster
- Kimcherrain Fuller
- Kimberly A. Gardner
- Mandana Ghashghaei
- Tricia Gilbreth
- Alexis N. Goolsby
- Latrina M. Gregory
- Nicole Griffith
- Nicotra M. Harris
- Lindsey Haynes
- Roy E. Heard
- Jennifer L. Jones
- Siraz A. Karatela
- Dustin M. Kemptner
- Renee A. Little
- Lynette S. Lord
- Jeffrey A. Martin
- Susan E. Martin
- Monique R. Morrison
- Aniema P. Ndem
- Kathy C. Nguyen
- Jennifer H. Parr
- Palek S. Patel
- Yvette M. Pavone
- James A. Pyle
- Bianca J. Roberson-Wright
- Wanda L. Robertson
- Karen Sailors
- Susan M. Seeba
- Sheretta L. Sinkfield
- Darrell D. Starks

- Jamie L. Starks
- Gerren R. Taylor
- Tomekia L. Trimble
- Barbara A. Vankempen
- William E. Waggaman
- Miranda A. Waltman
- Caitlin Whatley
- Keosha S. Williams
- Shourong-Zhao
- Diane Zimmerman

152. Boback and Tiversa's tortious interference was aimed at LabMD's existing contracts with third party payors, including those listed on Exhibit B hereto. Tiversa was aware of most of these relationships because Tiversa took a LabMD file that listed most of its third party payors.

153. Boback and Tiversa's tortious interference was aimed at the relationships LabMD had with insurance carriers. For example, The Hartford refused to renew a LabMD's comprehensive general liability ("CGL") policy effective May 5, 2014, due to the Enforcement Action, which was predicated on Tiversa and Boback's False Statements Regarding Disclosure, Source and Spread. Markel Insurance refused to renew its CGL and malpractice policies on LabMD, due to the Enforcement Action, which was predicated on Tiversa and Boback's False Statements Regarding Disclosure, Source and Spread.

154. Boback and Tiversa's tortious interference was aimed at LabMD's prospective contracts including, without limitation, the future relationships LabMD would have had with the aforementioned employees and others.

155. Boback and Tiversa's tortious interference was aimed at LabMD's prospective contracts including, without limitation, the future relationships LabMD would have had with the aforementioned third party payors and others.

156. Boback and Tiversa's tortious interference was aimed at LabMD's prospective contracts including, without limitation, the future relationships LabMD would have had with the aforementioned insurance carriers and others. OneBeacon, for example, refused to provide LabMD with ERP (extended reporting period) coverage to cover future malpractice claims because of the FTC investigation and Enforcement Action, which were predicated on Tiversa and Boback's False Statements Regarding Disclosure, Source and Spread. LabMD has not been able to obtain and no longer has medical malpractice coverage due to the False and Defamatory Statements Regarding Disclosure, Source and Spread.

CAUSES OF ACTION

~~**COUNT I: CONVERSION**~~
~~**(Against all Defendants)**~~

38. [Deleted.]

39. [Deleted.]

40. [Deleted.]

COUNT II: DEFAMATION *PER SE*
(Against all Defendants)

~~41. LabMD reincorporates each of the foregoing paragraphs as if they were fully set forth herein.~~

~~42. Defendants published the Defamatory Statements without privilege.~~

~~43. Defendants made the Defamatory Statements without regard to the truth of the statements, or in the alternative, made such statements out of malice towards LabMD.~~

~~44. Pursuant to both Pennsylvania and Georgia law, the Defamatory Statements constitute defamation *per se*.~~

~~45. LabMD's reputation was damaged as a result of the Defamatory Statements.~~

~~46. LabMD has suffered, and is continuing to suffer, damages and loss of business relationships as a result of the Defamatory Statements.~~

~~47. LabMD is entitled to recover damages from Defendants for this defamation *per se* in an amount to be proven at trial.~~

157. LabMD reincorporates each of the foregoing paragraphs as if they were fully set forth herein.

158. The Defamatory Statements Regarding Disclosure, Source and Spread made by Defendants (Defamatory Statement Nos. 1-20), are defamatory in character as they have diminished LabMD's reputations and have hurt LabMD's business by, inter alia, casting doubt on LabMD's operations as a business that operates legally, ethically and honestly.

159. Defendants published the Defamatory Statements Regarding Disclosure, Source and Spread in several publications, including the Wall Street Journal and the Pathology Blawg, to several individuals, including the FTC investigators, and to the FTC.

160. The Defamatory Statements Regarding Disclosure, Source and Spread are directly applicable to LabMD as they either name LabMD or make clear reference, in context, to LabMD.

161. Any recipient of the Defamatory Statements Regarding Disclosure, Source and Spread would understand the defamatory meaning of those statements.

162. Any recipient of the Defamatory Statements Regarding Disclosure, Source and Spread would understand these statements are to be applied to LabMD, as LabMD is either named or implicated in context.

163. There is no conditionally privileged occasion that exists to allow Defendants to have made the Defamatory Statements Regarding Disclosure, Source and Spread. In the

alternative, Defendants, as demonstrated above, have abused a conditionally privileged occasion to the extent any exist, which LabMD denies.

164. Defendants knew, or reasonably should have known, of the falsity of each of the Defamatory Statements Regarding Disclosure, Source and Spread at the time those statements were made. Defendants have acted with actual malice.

165. Defendants made the Defamatory Statements Regarding Disclosure, Source and Spread knowing, or reasonably should have known, and intending, that their publication would result in pecuniary loss to LabMD as a result of, inter alia, the negative effect the statements would have on LabMD's reputation.

166. Defendants' conduct, as described above, is outrageous, and demonstrates intentionally willful, wanton and reckless behavior on Defendants' part. Defendants had an appreciation for, and consciously disregarded, the risk of harm to LabMD, which their conduct entailed.

167. Pursuant to both Pennsylvania and Georgia law, the Defamatory Statements Regarding Disclosure, Source and Spread constitute defamation *per se*.

168. LabMD's reputation was damaged as a result of the Defamatory Statements Regarding Disclosure, Source and Spread.

169. LabMD has suffered special harm as a result of the publication of the Defamatory Statements Regarding Disclosure, Source and Spread.

170. LabMD has suffered, and is continuing to suffer, damages and loss of business relationships as a result of the LabMD's reputation was damaged as a result of the Defamatory Statements Regarding Disclosure, Source and Spread.

171. LabMD has suffered special harm as a result of the publication of the Defamatory Statements Regarding Disclosure, Source and Spread.

172. LabMD is entitled to recover damages from Defendants for this defamation *per se* in an amount to be proven at trial.

COUNT III: TORTIOUS INTERFERENCE WITH EXISTING AND PROSPECTIVE BUSINESS RELATIONSHIPS ~~BUSINESS RELATIONS~~
(Against all Defendants)

174. LabMD reincorporates each of the foregoing paragraphs as if they were fully set forth herein.

175. By engaging in the above described misconduct, Defendants have substantially harmed and/or seriously jeopardized LabMD's reputation and goodwill in the healthcare industry and its existing and prospective business relationships with employees, patients, providers, third party payors, insurance carriers, referral sources and others.~~patients, referral sources, and others.~~

176. Defendants knew or should have known that the above described misconduct would substantially harm and/or seriously jeopardize LabMD's reputation and goodwill in the healthcare industry and its existing and prospective business relationships with employees, patients, providers, third party payors, insurance carriers, referral sources and others.~~patients, referral sources, and others.~~

177. Defendants are strangers to these business relationships.

178. In acting in the manner described above, Defendants acted improperly, without privilege, purposely, and with malice and intent to injure LabMD.

179. As the proximate result of Defendants' interference with its business relationships, LabMD has been damaged in an amount to be proven at trial.

COUNT IV: FRAUD

(Against all Defendants ~~Tiversa and Boback~~)

180. LabMD reincorporates each of the foregoing paragraphs as if they were fully set forth herein.

181. In order to induce LabMD to obtain its services, Tiversa and Boback falsely told LabMD, among other things, that Tiversa had obtained the 1718 File from a peer-to-peer network and that Tiversa "continued to see individuals … downloading copies of the [1718 File]."

182. At the time Tiversa and Boback made these knowingly false statements, they intended to mislead and had actual knowledge that they were deliberately misleading LabMD.

183. Tiversa and Boback's actions in making knowingly false statements to LabMD were willful, wanton, outrageous, and in conscious disregard of LabMD's rights under law.

184. LabMD justifiably relied on the representations of Tiversa and Boback, primarily because they professed to be experts in the field of cyber security.

185. LabMD's good faith reliance on these misrepresentations was to its detriment because it spent thousands of dollars, and devoted hundreds of man hours, to seek to detect and remedy the phantom data breaches intentionally and fraudulently manufactured by Tiversa and Boback.

186. As a direct and proximate result of the fraudulent misrepresentations of Tiversa and Boback, LabMD has suffered damages in an amount to be proven at trial.

COUNT V: NEGLIGENT MISREPRESENTATION
(Against all Defendants ~~Tiversa and Boback~~)

187. LabMD reincorporates each of the foregoing paragraphs as if they were fully set forth herein.

188. Tiversa and Boback were negligent and failed to disclose material facts to LabMD by falsely representing to it that, among other things, Tiversa had obtained the 1718 File from a peer-to-peer network and that Tiversa "continued to see individuals … downloading copies of the [1718 File]."

189. Tiversa and Boback knew or should have known that the foregoing and above described representations were false when made.

190. Tiversa and Boback had a duty to refrain from making the foregoing and above described false representations.

191. Tiversa and Boback each breached their respective duty by making the foregoing and above described false representations.

192. It was reasonably foreseeable to Tiversa and Boback that LabMD would rely on such false or incomplete information, and LabMD did so to its detriment.

193. As a direct and proximate result of the negligent misrepresentations of Tiversa and Boback, LabMD has suffered, and is continuing to suffer, substantial damages.

194. Accordingly, LabMD is entitled to damages for the negligent misrepresentations of Tiversa and Boback in an amount to be proven at trial.

COUNT VI: CIVIL CONSPIRACY
(Against all Defendants)

195. LabMD reincorporates each of the foregoing paragraphs as if they were fully set forth herein.

196. Defendants have a common design and purpose to achieve their goal of commercially benefitting from misrepresentations about data security breaches, which specifically harmed LabMD through Defendants': (i) conversion of LabMD's property; (ii)

Defamatory Statements relating to LabMD's trade and profession; and (iii) interference with LabMD's business relations.

197. Defendants have acted in concert with an unlawful, malicious, and willful common purpose, and with unlawful means, to: (i) convert LabMD's property; (ii) defame LabMD; and (iii) interfere with LabMD's business relations.

198. Defendants took overt acts in furtherance of this unlawful, conspiracy.

199. LabMD has sustained damages as a direct and proximate result of Defendants' unlawful conspiracy. These damages include loss of profits and damage to and loss of its reputation and goodwill.

200. Defendants' actions are a direct and proximate cause of significant harm to LabMD.

201. Defendants are jointly and severally liable to LabMD for damages in an amount to be proven at trial.

~~**COUNT VII: VIOLATION OF RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT ("RICO"), 18 U.S.C. § 1962(c) (Against all Defendants)**~~

202. [Deleted.]

203. [Deleted.]

204. [Deleted.]

205. [Deleted.]

206. [Deleted.]

207. [Deleted.]

208. [Deleted.]

209. [Deleted.]

210. [Deleted.]

211. [Deleted.]

212. [Deleted.]

213. [Deleted.]

214. [Deleted.]

~~**COUNT VIII: VIOLATION OF RICO, 18 U.S.C. § 1962(d)**~~
~~**(Against all Defendants)**~~

215. [Deleted.]

216. [Deleted.]

217. [Deleted.]

218. [Deleted.]

COUNT IX: PUNITIVE AND TREBLE DAMAGES
(Against all Defendants)

219. LabMD reincorporates each of the foregoing paragraphs as if they were fully set forth herein

220. Based on the facts as set forth above, Defendants' actions have demonstrated willful misconduct, malice, fraud, wantonness, oppression, or that entire want to care which would raise the presumption of conscious indifference to consequences. Defendants have further acted with specific intent to cause LabMD harm. Accordingly, LabMD is entitled to an award of punitive damages against Defendants.

221. LabMD is additionally entitled to a compulsory award of treble damages as a result of Defendants' RICO violations.

COUNT X: ATTORNEYS' FEES AND EXPENSES OF LITIGATION
(Against all Defendants)

222. LabMD reincorporates each of the foregoing paragraphs as if they were fully set forth herein.

223. LabMD is entitled to recovery of its attorneys' fees and court costs pursuant to 18 U.S.C. § 1964(c).

224. Moreover, Defendants have acted in bad faith toward LabMD in the events giving rise to this lawsuit, have been stubbornly litigious, and have put LabMD to unnecessary trouble and expense. Pursuant to Georgia law, O.C.G.A. § 13-6-11, LabMD is entitled to recover from Defendants its expenses of litigation, including reasonable attorneys' fees in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, LabMD, Inc. respectfully prays for the following relief:

(a) that LabMD receive a trial by jury;

(b) that the Court enter judgment in favor of LabMD, and against Defendants, jointly and severally, on Counts II~~I~~-III and VI~~II~~-X of the Complaint, in amount(s) to be proven at trial, including awarding against each Defendant actual, special, consequential and/or compensatory damages, including lost profits;

(c) that the Court enter judgment in favor of LabMD, and against Boback and Tiversa, jointly and severally, on Counts IV-V of the Complaint, in amount(s) to be proven at trial, including awarding against each Defendant~~Boback~~ actual, special, consequential and/or compensatory damages, including lost profits;

(d) that judgment be entered awarding to LabMD, and against each Defendant, punitive damages;

(e) that judgment be entered awarding to LabMD, and against each Defendant, enhanced and/or treble damages;

(f) that LabMD be awarded its expenses and costs and disbursements of litigation, including its costs and reasonable attorneys' fees;

(g) that LabMD be awarded pre-judgment and post-judgment interest as provided by Pennsylvania and/or Georgia law; and,

(h) that LabMD be awarded such other relief as the Court deems just, equitable and proper.

JURY TRIAL DEMANDED.

Respectfully submitted,

Dated: February 12, 2016

DUANE MORRIS LLP

/s/Kenneth M. Argentieri
Kenneth M. Argentieri
Pa. I.D. No. 41468
DUANE MORRIS LLP
600 Grant Street, Suite 5010
Pittsburgh, PA 15219
V: 412-497-1005
F: 412-202 0669
kmargentieri@duanemorris.com

JAMES W. HAWKINS, LLC

/s/ James W. Hawkins
James W. Hawkins
Admitted pro hac vice
Georgia State Bar No. 338767
JAMES W. HAWKINS, LLC
11339 Musette Circle
Alpharetta, GA 30009
V: 678-697-1278
F: 678-540-4515
jhawkins@jameswhawkinsllc.com

Attorneys for Plaintiff LabMD, Inc.